Computer Search and Seizure & The Law of Interrogations

Orin Kerr

Professor of Law

George Washington University

Topics

- 2 Hours on Computer Search and Seizure
  - What is a search and seizure of computer data?
  - Searches of Computers With a warrant
  - Searches of Computers Without a warrant

- 1 Hour on *Miranda* and the Law of Police Interrogations

Computer Search and Seizure

- Electronic information often useful to criminal cases! Computers keep lots of records of what people do.
  - Child pornography images
  - E-mails that disclose a fraud scheme
  - Evidence of search queries relevant to a crime
  - Drafts of ransom notes
  - Deleted files showing use of specific programs or downloading specific information
  - Cell phone records that show location

Question: What are the rules that govern access to that information?

Fourth Amendment Overview

- Prohibits Unreasonable Searches and Seizures
  - Searches: Reasonable Expectation of Privacy test
  - Seizures: Interference with Possessory Interest
- If a search or seizure occurs, it is reasonable and therefore constitutional only if (a) a valid warrant was obtained or (b) an exception to the warrant requirenebt applies.

Computers are Private

- “Because intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.”
  - United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007).

Retrieving Data as a Search

- Retrieving data from a computer is ordinarily a “search” of that computer.
- Container analogy: Accessing a file on a computer is like opening a container.
  - See Andrus
  - U.S. v. Runyan, 275 F.3d 449 (5th Cir. 2001).
- So long as person has a reasonable expectation of privacy in the computer, opening the file violates the person’s reasonable expectation of privacy.

General Exceptions

- No reasonable expectation of privacy in a stolen computer.
  - United States v. Caymen, 404 F.3d 1196 (9th Cir. 2005).
- No reasonable expectation of privacy if data already observed by police.
  - If police see something and write about it and put the info in a computer, it's not protected by an REP.
  - Illinois v. Andreas, 463 U.S. 765, 771-72 (1983).

Special Case: Computer Networks

- E-mail stored on a server, contents of password-protected website protected.
  - Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008).
  - United States v. D'Andrea, 497 F.Supp. 117 (D. Mass. 2007).
- Non-content information, files made available to the public not protected.
  - United States v. Forrester, 495 F.3d 1041 (9th Cir. 2007)
  - United States v. Gines-Perez, 214 F.Supp.2d 205 (D.P.R. 2002).
  - United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008).

Seizures of Computers

- Seizure is “some meaningful interference with an individual’s possessory interest” in the property.
    - United States v. Jacobsen, 466 U.S. 109, 113 (1984).
- Taking away the physical device seizes it.
- But what about merely copying data and leaving the original behind? Does that “seize” anything?

Answer is Uncertain!

- View One: Copying is a seizure because it takes away exclusive control over data.
    - United States v. Jefferson, 571 F.Supp.2d 696 (E.D.Va. 2008).
- View Two: Copying is not a seizure because it doesn't take anything away.
    - In re United States, -- F.Supp.2d ----, 2009 WL 3416240 (D.Or. 2009)
- My Answer: Copying is normally a seizure. See *Fourth Amendment Seizures of Computer Data*, Yale L.J. (forthcoming 2010) (available in draft at ssrn.com)

Summary of Search and Seizure

- In most circumstances, looking inside an electronic storage device is a *search* and copying computer data is a *seizure*.
- More broadly, collection of computer data by the government will often trigger Fourth Amendment protection.

Warrant Searches

- Warrants are court orders that allow the government to go to a particular place and take particular things that are evidence, contraband, fruits, or instrumentalities of crime.
- “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const Amend IV.

Two Stages of Computer Warrants

- Stage One: Physical Search Stage
  - Government goes to place and takes away computers.
  - Government brings seized computers back to lab and makes an “image” copy.
- Stage Two: Electronic Search Stage
  - Government searches the “image” copy for evidence, coming across a great deal of information along the way.

Facial Validity

- Probable cause.
  - Fair probability to think that data or item would be somewhere in the place to be searched. U.S. v. Gourde, 440 F.3d 1065 (9th Cir. 2006).
- Particularity.
  - "All computers" is not acceptable: Need to say all computers containing a particular kind of evidence. U.S. v. Riccardi, 405 F.3d 852 (10th Cir. 2005).
  - Searches for physical writings generally cover writings in electronic form. People v. Gall, 30 P.3d 145 (Colo. 2001).

Physical Search Stage

- Seize first, search later requires seizing more than just evidence. Agents go in and often take all the computers, without knowing which ones may contain the evidence. Courts have widely allowed on reasonableness grounds.
    - U.S. v. Schandl, 947 F.2d 462 (11th Cir. 1991).
- Ninth Circuit has allowed but said the warrant affidavit must explain the need for the over-seizure.
    - U.S. v. Hill, 459 F.3d 966 (9th Cir. 2006).

Electronic Search Stage

- Agents look through computer and find evidence. Evidence within scope of warrant admitted, even if it is a deleted file.
    - U.S. v. Upham, 168 F.3d 532 (1st Cir. 1999).
- Evidence outside warrant admitted only if in plain view. Test for plain view has tended to be subjective, not objective: Was agent intending to comply with the warrant when he came across evidence?
    - U.S. v. Carey, 172 F.3d 1268 (10th Cir. 1999).

Search Protocols

- Some courts have considered or imposed search protocols for how warrant executed as a way to ensure the warrant is executed narrowly.
    - In re Search of 3817 W. End, 321 F.Supp.2d 953 (N.D. Ill. 2004).
- Most courts have rejected this, though, on ground that warrants govern what and when search occurs but not how.
    - Upham, 168 F.3d at 537. U.S. v. Brooks, 427 F.3d 1246 (10th Cir. 2006.)

CDT – 9th Circuit Revolution!

- Blockbuster en banc decision rewrites the rules! **U.S. v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. Aug 26, 2009).**
- Magistrates must impose limits on computer warrants ex ante, including 1) Requiring waiver of plain view; 2) taint teams; 3) search protocols; 4) destruction or return of evidence; and 5) whatever else the magistrate wants to impose.
- But will it stand? *And will any other court follow?*

New Fed. R. Crim. Pro. 41

- Effective 12/09, Amendments that specifically deal with computer search and seizure.
- “A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.”
- “In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied. ”

Exceptions to Warrant Requirement

- Most computer searches and seizures are warrantless.
- Major exceptions include:
  - Exigent circumstances
  - Consent
  - Search Incident to Arrest
  - Border Searches
  - Government workplace searches

Exigent Circumstances

- Electronic evidence can be easily destroyed, and reason to think it will be justifies its warrantless seizure (although not its search) as reasonable.
  - U.S. v. Trowbridge, 2007 WL 4226385 (N.D. Tex. 2007) (hackers knew police were coming)
  - U.S. v. David, 756 F. Supp. 1385 (D. Nev. 1991) (officer saw suspect start to delete files, but couldn’t search based on belief battery might fade.)

Consent

- Voluntary consent by one who can consent.
- Scope of consent: What a “typical reasonable person” would think.
    - U.S. v. Al-Marri, 230 F. Supp. 2d 535 (S.D.N.Y. 2002).
    - Often in flux with new technologies.
- Withdrawn consent: What if suspect consents, copy is made, *then* suspect withdraws consent?
    - U.S. v. Megahed, 2009 WL 722481 (M.D. Fla. 2009).

Third-party and Apparent Consent

- When computers are shared, sharer can consent to search. But can't consent to search of password-protected files.
  - U.S. v. Buckner, 473 F.3d 551 (4th Cir. 2007).
- Government can search based on "apparent" third-party consent, if reasonable officer would think there was consent. But computer forensic software can bypass passwords!
  - U.S. v. Andrus, 483 F.3d 711 (10th Cir. 2007).

Search Incident to Arrest

- What if suspect has a cell phone or computer on his person when arrested? Can governmentt search it as part of arrest power, like it can search wallets and packages?
- Cell phone searches incident to arrest generally upheld.
    - U.S. v. Murphy, 552 F.3d 405 (4th Cir. 2009).
- Some courts limit to searches at the time of arrest, however, suggesting other possible limits in future cases.
    - U.S. v. Park, 2007 WL 1521573 (N.D. Cal. 2007).

Border Searches

- Courts have allowed complete searches of computers at the border.
  - U.S. v. Arnold, 533 F.3d 1003 (9th Cir. 2008).
- However, some courts have suggested limitations on where and when search can occur.
  - U.S. v. Cotterman, 2009 WL 465028 (D. Ariz. 2009), presently on appeal, invalidating border search when computer sent to forensic agent away from border for search.

Government workplace computers

- First, was a banner or warning in place that eliminated privacy rights?
- If not, was the search "reasonable" in light of legitimate workplace needs?
  - Leventhal v. Knapek, 266 F.3d 64 (2d. Cir. 2001) (Sotomayor, J.)
- Government normally uses banner to obtain waiver of rights, and that ends the issue.
  - Usually, but not always found to waive rights. For an exception, see Quon v. Arch Wireless (9th Cir. 2008).

Where to Learn More

- U.S. Department of Justice Treatise on Computer Search and Seizure, free on the web!
- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d. Ed. 2009)
- http://www.cybercrime.gov/ssmanual/index.html

The Law of Interrogations

- “You have a right to remain silent. Everything you say can and will be used against you in a court of ……”
- Wait, I’ll bet you know that part!
- The complex law of *Miranda v. Arizona*, and the various stages of *Miranda* law.

Pre-Miranda Law

- At common law, confessions had to be voluntary.
- Voluntariness test becomes part of Due Process, but courts have a very hard time saying when a confession is voluntary.
- A trial judge could write findings to make almost anything seem voluntary.

The *Miranda* Answer

- Miranda v. Arizona, 384 U.S. 436 (1966).
- Before custodial interrogation can occur, a suspect 1) must be informed of his rights and 2) must waive his rights.
- Basic idea: replace uncertain voluntariness test with a relatively clear process of warning and then waiver.

Custodial Interrogation

- Miranda warnings and waiver required only under custodial interrogation.
- Custody: Reasonable person would not feel free to leave. Either under arrest or similar state.
    - Yarborough v. Alvarado, 541 U.S. 652 (2004).
- Interrogation: Express questioning or “any words or action that the police should know are reasonably likely to elicit an incriminating response.”
    - Rhode Island v. Innis, 446 U.S. 291 (1980).

What Warnings, What Waiver?

- Warnings must convey basic meaning of Miranda rights.
  - Duckworth v. Eagan, 492 U.S. 195 (1989).
  - Florida v. Powell, argued at SCT two weeks ago.
- Govt must satisfy “heavy burden” of waiver. Must show actual waiver, not merely proceeding after warnings provided, before interrogation can stop.
  - N.C. v. Butler, 441 U.S. 369 (1979).
  - Tague v. Louisiana, 444 U.S. 469 (1980).
  - Initials and signing form almost always enough.

When Suspects Assert Their Rights

- Clear statement that a suspect wants to talk to a lawyer stops everything. Suspect must be provided a lawyer, and the government cannot interrogate the suspect outside the presence of an attorney so long as he is in custodial interrogation unless the suspect initiates the conversation.
    - Edwards v. Arizona, 451 U.S. 477 (1981).
    - Oregon v. Bradshaw, 462 U.S. 1039 (1983) (reinitiation).
    - Davis v. United States, 512 U.S. 452 (1994) (clear statement)
- Right to remain silent also must be respected, although police can eventually ask again.
    - Michigan v. Mosley, 423 U.S. 96 (1975).

Miranda Exceptions

- Court often balances Miranda rights versus other rights and interests, carving out exceptions to Miranda.
  - Public safety. New York v. Quarles, 467 U.S. 649 (1984).
  - Jail plant – undercover agent acting as fellow prisoner. Illinois v. Perkins, 496 U.S. 292 (1990).
  - Routine booking exception. Pennsylvania v. Muniz, 496 U.S. 582 (1990).

Miranda Remedies

- No fruit of the poisonous tree doctrine!
- Following warning/waiver procedure generally allows evidence.
  - Oregon v. Elstad, 470 U.S. 298 (1985).
  - But see Missouri v. Seibert, 542 U.S. 600 (2004) (different rule for intentional two-step).
- Even if Miranda not followed, physical fruits not excluded; only the statements excluded.
  - U.S. v. Patane, 542 U.S. 630 (2004).

•Questions?

- For more, see Wayne LaFave, et. al., Criminal Procedure (3d Ed. 2007).
- Available on WESTLAW as CRIMPROC database.